IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Messaoud Benantar		
Assignee:	International Business Machines Corporation		
Title:	Method and System for Public-Key-Based Secure Authentication to Distributed Legacy Applications		
Serial No.:	09/821,079	Filing Date:	March 29, 2001
Examiner:	Christopher J. Brown	Group Art Unit:	2134
Docket No.:	AUS920010064US1	Customer No.	65362

Austin, Texas
August 25, 2008

FILED ELECTRONICALLY

REPLY BRIEF UNDER 37 CFR § 41.41

Dear Sir:

Applicant submits this Reply Brief in response to the Examiner's Answer mailed in this case on June 23, 2008. This reply will address selected arguments from the Examiner in the "Response to Argument" section of the Examiner's Answer, but will not attempt to address every argument since Applicant's Appeal Brief has previously addressed the appeal issues. It is believed that no fees are due in connection with the filing of this Reply Brief, however, the Commissioner is authorized to deduct any amounts required for this Reply Brief and to credit any amounts overpaid to Deposit Account No. 090447.

Regarding the obviousness rejection of the pending claims, Applicant respectfully submits that the claim requirement of using an "attribute certificate" to convey encrypted authentication data has not been disclosed or suggested by the prior art. In particular, the Examiner relies on Wood's disclosure at column 18, lines 35-55 and Figure 4 to meet the claim requirement of "extracting encrypted authentication data from the attribute certificate" and then "decrypting the encrypted authentication data to regenerate the authentication data." Examiner's Answer, p. 9. While this passage from Wood refers to encoding login credentials (such as a password, certificate, biometric results, Enigma challenge response) in the "login credentials structure 410" with a public key, the

Examiner appears to be confusing Wood's public key certificate process with the claimed "attribute certificate" requirement. As explained by Applicant in the application, an "attribute certificate" differs from a public key certificate in both structure and function. *See*, Application, page 19, line 20 to page 21, line 23. In the field of computer security, an attribute certificate (also known as an authorization certificate) is a digital document that describes a written permission from the issuer to use a service or a resource that the issuer controls or has access to use. These differences between a public key certificate (PKC) and attribute certificate (AC) are addressed by the relevant IETF protocol statement:

> Some people constantly confuse PKCs and ACs. An analogy may make the distinction clear. A PKC can be considered to be like a passport: it identifies the holder, tends to last for a long time, and should not be trivial to obtain. An AC is more like an entry visa: it is typically issued by a different authority and does not last for as long a time. As acquiring an entry visa typically requires presenting a passport, getting a visa can be a simpler process.

S. Farrell et al., "An Internet Attribute Certificate Profile or Authorization," RFC 3281 (April 2002) (http://tools.ietf.org/html/rfc3281). *See also*, Wikipedia, Authorization Certificate, http://en.wikipedia.org/wiki/Authorization_certificate (August 25, 2008). Based on Applicant's review, there is no teaching or suggestion by Wood, either alone or in combination with the other cited references, of including encrypted authentication data in an attribute certificate that the encrypted login credentials are conveyed within "an attribute certificate" as claimed.

For at least the foregoing reasons, Applicant respectfully submits that a *prima facie* case of obviousness has not been established because neither Wood nor Perlman (nor any of the other cited references) disclose or suggest using an "attribute certificate" to convey encrypted authentication data. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection because the Examiner has not established a *prima facie* case of obviousness by showing that all the claim limitations are taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974); In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Accordingly, claims 1, 14, and 25 are allowable. To the extent that the pending dependent claims each respectively incorporate the requirements of independent claims 1, 14, and 25, these dependent claims are likewise allowable, even though there are additional differences

recited in the dependent claims. Accordingly, Applicant requests that the obviousness rejections of claims 1-7, 14-20, and 25-31 be withdrawn and that the claims be allowed.

CONCLUSION

A *prima facie* case of obviousness has not been established because none of the cited references discloses Applicant's use of an attribute certificate to convey encrypted authentication data to a host for authenticating a client seeking to access a controlled resource. In view of the above arguments, it is respectfully urged that the rejection of the claims should not be sustained.

CERTIFICATE OF TRANSMISSION

I hereby certify that on August 25, 2008 this correspondence is being transmitted via the U.S. Patent & Trademark Office's electronic filing system.

/Michael Rocco Cannatti/

Respectfully submitted,

/Michael Rocco Cannatti/

Michael Rocco Cannatti
Attorney for Applicant(s)
Reg. No. 34,791